

Department of Technology Services (DTS) – Security Requirements

DTS

- Attached to every IAA (Interagency Agreement) with Department of Technology Services (DTS) is a 'security compliance' exhibit. The IAA is issued on a fiscal year basis every year.
- Any specific discussions related to infrastructure or architecture as implemented by Department of Technology Services (DTS), other than the fact that we use DMZ and firewalls, is reserved for confidential discussions.

State

- SAM 4800 and subsection 4841 specifically (<http://www.dgs.ca.gov/Publications/default.htm> - State Administrative Manual (SAM));
- ISO 17799 (<http://www.securityauditor.net/iso17799/>);
- Federal Information Processing Standards (<http://csrc.nist.gov/publications/fips/>).

SECURITY COMPLIANCE STATEMENT

Entities requesting to connect their networks or their network devices to Teale Data Center network or resources accessible on Teale's network, must comply with the following basic information security requirements. These requirements will be included in any Agreement or contract with an entity that includes the provision of connectivity to Teale or a resource accessible on Teale's network.

- A. **Firewalls** - This requirement provides a reliable mechanism to help protect Teale and it's customers' information and information processing resources from unauthorized access to, and denial/disruption of services or systems.
- **Definition** - A firewall is a computer or system of computers designed to restrict network traffic in order to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, but are strongest when implemented as a hardware/software combination.
 - **Requirements** - Any network used by a customer to connect to Teale information resources will be protected by at least one firewall system properly situated to examine traffic between the network and each external network entry point. The customer shall ensure that firewalls include, at a minimum, provisions for packet filtering, application gateway security mechanisms, and circuit-level gateways.
- B. **Physical Security** - This requirement ensures that the hardware that permits network access to Teale Data Center is adequately protected to prevent harm to the physical components that enable connectivity between the customer's network and Teale Data Center.
- **Definition** - Physical Security involves measures taken to prevent physical access, which may allow loss of or damage to, the system or the information stored on it.
 - **Requirements** - Physical access to network components, servers, and data storage components used in conjunction with access to Teale Data Center information resources should be limited to the appropriate designated staff who implement and maintain the components.
- C. **Access Control** - This requirement ensures that policies, procedures and technology mechanisms are in place for Teale's customers only to limit access to the Teale Data Center's network and the information resources in Teale's custody to those authorized individuals or entities.
- **Definition** - Access control includes processes and systems to determine which system resources, application functions and information must be restricted to certain customers, business partners, and contractors and to allow access by those customers while preventing access by others.
 - **Requirements** - Access to information designated as private or confidential must be limited to those individuals or entities specifically authorized to access that information. Access to system functions and processes under Teale Data Center's custody that can affect the availability, functionality or security of departmental information or information resources should be restricted to those individuals who require that access in order to perform duties essential to the operation and maintenance or use of that system.

Teale is requiring Security Compliance for audit purposes.

- ☐ Customer is in full compliance with the aforementioned security requirements.
- ☐ Customer is not in full compliance, however, will contact Teale's Information Security Officer at 916-464-3672 to develop a plan of action for compliance with the security requirements.
- ☐ N/A - Customer does not have a network connection to Teale Data Center.

Information Security Officer Signature

Date